

**ЈЕЛЕНА МАТИЈАШЕВИЋ\***

**ЈОКО ДРАГОЈЛОВИЋ\*\***

Правни факултет за привреду и правосуђе  
Нови Сад

UDC: 343.3/.7:343.98

Прегледни рад

Примљен: 21.09.2021

Одобрен: 09.11.2021

Страна: 51–63

DOI: 10.51738/Kpolisa2021.18.2p.1.04

## **МЕТОДИКА ОТКРИВАЊА КРИВИЧНИХ ДЕЛА РАЧУНАРСКОГ КРИМИНАЛИТЕТА**

**Сажетак:** Рачунарски криминалитет карактерише изузетна феноменолошка разноврсност која отежава његово јединствено и прецизно појмовно одређење, а перманентан интензивни развој рачунарских технологија доприноси константном проширивању појавних облика и поставља све веће изазове пред органе надлежне за његово сузбијање. Након краћег осврта на појам и значај криминалистике као науке, и криминалистичке методике као гране криминалистике, те појмовног одређења и основних карактеристика криминалитета уопште, и рачунарског криминалитета, у раду су анализирани најзначајнији аспекти методике откривања кривичних дела из ове области. Закључак је да основне карактеристике рачунарског криминалитета, отежано откривање, компликовано доказивање и неефикасна превенција свакако подстичу потенцијалне извршиоце на доношење одлуке о предузимању радњи кривичних дела из ове области, што опет упућује на то у ком смеру се треба кретати у циљу отклањања потешкоћа у методици откривања и прикупљања доказа код кривичних дела рачунарског криминалитета.

**Кључне речи:** рачунарски криминалитет, криминалистика, криминалистичка методика, Кривични законик, кривична дела

### **Увод**

Општа је претпоставка да се у савременим условима живота информатичка писменост великог броја људи једноставно подразумева. Развој информационах и комуникационих технологија „сасвим извесно представља најбрже напредовање једне нове технологије, у историји човечанства икада виђено” (Радовић 2008, 129.). Тај процес је за собом донео и „велике промене у готово свим областима живота и рада савременог човека” (Матијашевић, Бингулац и Драгојловић 2015, 393).

\* jelena@pravni-fakultet.info

\*\* jdragojlovic@pravni-fakultet.info

Упоредо са развојем информатичке писмености и овладавањем техника рада на рачунару, повећавају се и могућности манипулативног коришћења рачунарских технологија. Данас се рачунарска технологија може употребити, али и злоупотребити на различите начине. Поред законом одређених кривичних дела против безбедности рачунарских података, било који вид традиционалног криминалитета (на пример: крађе, утаје и проневере, и др.) може се реализовати помоћу компјутера, док се подаци који се неовлашћено прибављају злоупотребом рачунарских технологија могу на различите начине користити за стицање противправне користи.

Према Бановићу (2002), „данас компјутери суверено владају најважнијим сегментима и процесима друштвеног и економског живота” (129). Међутим, „истина је да не постоји техничко и технолошко достигнуће које у историји човечанства није наишло на различите видове злоупотреба” (Матијашевић 2013, 1). Такође, „са првим злоупотребама ове врсте, јављају се и прве реакције на ове противзаконите активности” (Матијашевић, Бјелајац и Димитријевић 2012, 37).

У ширем контексту, криминалитет је познат од самог настанка човечанства, и „друштвени је феномен који има више својих лица и налицја” (Матијашевић 2008, 81). У теорији се често истиче да „људско друштво од почетка свог настанка познаје начине понашања који се називају криминалитетом. Међутим, са развојем друштва и културе мењао се број и садржај кажњивих понашања, што упућује на закључак да криминалитет није статичан и фиксно одређен, те да се он стално мења” (Николић-Ристановић и Констатиновић-Вилић 2018, 21). Осим тога, „криминалитет представља и скуп друштвених појава којима се угрожавају универзалне друштвене вредности, а које су као такве санкционисане кривичним правом матичне државе” (Ђукић, 2019, 96).

У домену супротстављања криминалитета, криминалистика представља научну дисциплину усмерену ка пракси „која има веома битно место и улогу у области сузбијања криминалитета. Јер, предмет криминалистике јесте криминалитет, те је сходно томе криминалистика као наука изградила сопствене криминалистичке методе и средства, која су најпогоднија за сузбијање криминалитета (индиције, верзије, златна питања и др)” (Матијевић, Шушљик и Шарчевић 2020, 13). Имајући речено у виду, увек је интересно и значајно анализирати аспекте криминалистичке методике у откривању кривичних дела, јер ова грана криминалистике, осим што „прилагођава општа криминалистичко – тактичка правила специфичностима конкретних случајева” (Матијевић, Шушљик и Шарчевић 2020, 13), проучава „посебности и усавршава начине и методе за откривање и спречавање извршења одређене врсте, типа, групе кривичних дела” (Станковић 2016, 30).

Након краћег осврта на појам и значај криминалистике као науке, и криминалистичке методике као гране криминалистике, те појмовног одређења и основних карактеристика криминалитета уопште, и рачунарског криминалитета, биће анализирани аспекти методике откривања кривичних дела рачунарског криминалитета.

## **Појмовно одређење и значај криминалистике и криминалистичке методике**

Значајна научна дисциплина која своју практичну примену, у општем смислу, налази у борби против криминалитета, јесте криминалистика.

Криминалистика је, према свом примарном одређењу, „научна дисциплина која проналази, проучава и примењује научне или на практичном искуству засноване методе и средства, која су најпогоднија да се разјасни кривично дело, открије учинилац и обезбеде докази, као и да се спречи извршење будућих кривичних дела. Као и друге научне дисциплине, криминалистика има за циљ сузбијање криминалитета” (Станковић 2016, 18).

У практичном погледу, „криминалистика је сложена, информативна стратегија, која обухвата научне и на искуству засноване методе и средства за откривање, прикупљање, обрађивање, оцењивање и коришћење криминалистички релевантних информација, у циљу откривања, расветљавања и спречавања кривичних дела” (Алексић и Миловановић, 1991, 1). Предмет криминалистике је двострук: „а) ту спадају конкретна кривична дела и околности које наговештавају могућност наступања конкретног криминалног догађаја. Дакле, предмет криминалистике је криминалитет, његова свестрана анализа, као и настојање да се прикупи што више информација о кривичним делима и њиховим извршиоцима; б) криминалистика проналази и усавршава методе, усавршава средства, односно технику и радње које у пракси имају циљ да спрече и сузбијају развој криминалитета” (Станковић 2016, 21).

Према Матијевићу и сар. (2020), „развијајући се истовремено као научна и као практична дисциплина, криминалистика прихвата законитост и правила других наука, прилагођавајући их и непосредно их примењујући, а, у исти мах, изграђује и сопствене научне и на практичном искуству засноване методе и средства. На тај начин се стварају услови за успешно остваривање задатка које друштво, настојећи да се заштити од криминалитета, поверава криминалистички” (11).

У основи, „овај задатак се односи на остваривање следећих циљева: а) проучавање и евидентирање метода и средстава који се користе приликом планирања, припреме, вршења и прикривања кривичних дела; б) проучавање начина и метода долажења до почетних сазнања о припремању, односно извршењу кривичног дела; в) проналажење најефикаснијих метода расветљавања кривичних дела; г) проналажење најефикаснијих метода откривања и проналажења учинилаца кривичних дела; д) проналажење најефикаснијих и прилагођавање постојећих метода откривања, фиксирања и тумачења доказа о извршеном кривичном делу и кривици одређеног лица; ђ) изучавање и унапређење метода и средстава спречавања криминалитета за дужи временски период” (Матијевић и Марковић 2013, 1).

Криминалистику карактерише трипартитна подела грана које чине њен саставни део, коју је у наш правни систем још 1985. године унео проф. др Владимир Водинелић, а према којој се као посебни делови криминалистике издва-

јају: криминалистичка тактика, криминалистичка техника и криминалистичка методика. У теорији се последњих година као посебни делови криминалистике означавају криминалистичка стратегија и криминалистичка оператива.

Криминалистичка методика је, у основи, „посебни дио криминалистичке тактике, која се бави проучавањем посебности и усавршавањем начина и метода за откривање и спречавање извршења одређене врсте, типа, групе кривичних дела. Према томе, криминалистичке методике се баве оним што је битно за откривање, истраживање, доказивање и спречавање конкретног кривичног дела. Може се рећи да данас криминалистичке методике представљају збир свих криминалистичко-тактичких и криминалистичко-техничких знања, те њихову примену у откривању и расветљавању појединих кривичних дела” (Станковић 2016, 30).

Према Бошковићу и Бановићу (1995), „криминалистичка методика користи криминалистичко-тактичке и криминалистичко-техничке методе и средства, прилагођавајући их на поједина кривична дела, али изграђујући при томе своје сопствене методе, који се заснивају на специфичностима сваког типа кривичног дела” (5). Ђукић (2017) наглашава да се данас у пракси „суочавамо са чињеницом да се савремени облици криминалне делатности прилагођавају објективним условима, а савремена научна и техничка достигнућа користе се у функцији усавршавања појавних облика и начина извршења кривичних дела. Према томе, и методи супротстављања оваквом криминалитету морају се мењати и прилагођавати, проналазити нови и усавршавати већ познати, те конкретизовати по појединим кривичним делима. У том смислу, треба сагледати потребу за актуелношћу криминалистичке методике и као практичне делатности, али и као научне криминалистичке дисциплине” (142).

Предмет криминалистичке методике „чини изучавање појавних облика и начина извршења појединих кривичних дела, с једне стране, и праксе органа откривања и гоњења у спречавању и откривању тих кривичних дела, с друге стране” (Матијевић и Марковић 2013, 327). Даље, „пракса органа откривања и гоњења, а нарочито полиције, представља основу за утврђивање и усавршавање одређених правила поступања у конкретним ситуацијама извршених кривичних дела. Уопштавањем ове праксе, уз примену научних метода, долази се до правила чија је примена дала успешне резултате, али се истовремено одбацују они начини и методи рада који нису резултирали успехом у откривању и доказивању кривичних дела” (Ђукић 2017, 142). На тај начин, „криминалистичка методика изграђује се и као научна дисциплина, али и као практична делатност за сузбијање и спречавање појединих кривичних дела, што и јесте њен основни задатак” (Матијевић и Марковић 2013, 327).

## **Криминалитет – научни и друштвени контекст и појавни облици**

Одавно је постало јасно да се друштвена правила и норме не поштују увек. Људи их се најчешће придржавају (нарочито када је реч о тежим преступима) из страха од санкције. Међутим, немогуће је направити строгу поделу

грађана на оне који се придржавају успостављених правила и на оне који то не чине. Да ли ће неко извршити одређени деликт врло често зависи од околности у којима се то лице нашло, дотадашњег начина живота, од личних и породичних прилика, здравственог, финансијског, емотивног стања, и других околности.

Такође, „како ће се друштво поставити према одређеним девијантним понашањима појединаца (или група) зависи највише од менталитета, културолошког развоја, те става одређене заједнице према криминалних радњама. Поједнако опредељујући критеријуми су економска стабилност и политичка ситуација на одређеним локалитетима. У овом контексту се може рећи да оно што је стигматизовано и определено као деликт у једном друштву, не мора као такво бити одређено у другом друштву” (Матијашевић и Зарубица 2021, 29).

Криминалитет представља веома сложену појаву једнако штетну у свим друштвима и на свим нивоима развоја. Да би се схватио, „појам криминалитета мора се разматрати мултидисциплинарно” (Матијашевић 2012, 52). При овој констатацији, мора се нагласити да „мултидисциплинарност у приступу разматрања криминалитета није ствар избора, већ представља неопходан приступ овој сложеној друштвеној појави” (Бјелајац и Матијашевић 2014, 534).

Према Бјелајцу (2013), „опште прихваћена дефиниција криминала односи се на све оне активности (и пропуштања) које угрожавају у одређеном временском размаку поједина лица или пак добра – у материјалном и моралном смислу, која припадају тим појединцима, разним друштвеним органима и организацијама као и друштву узев у целини, а које су инкриминисане у важећим кривичноправним нормама једне земље, сматрају се и правно третирају као њен криминалитет за то време” (29). Дакле, криминалитет је сложена друштвена појава „детерминисана бројним чиниоцима везаним за субјект извршиоца, кривично дело и социјалну средину” (Бошковић и Марковић 2015, 155).

Криминалитет, „као негативна друштвена појава, може се поделити по разним основама, као нпр. по врсти делатности, објекту напада, старости учиниоца, степену организованости, и др., али је још увек најприхватљивија она подела криминалитета која га дели на општи, привредни, политички, и у новије време еколошки криминалитет, јер се у оквиру ње могу разврстати и поделе криминалитета по осталим критеријумима” (Бошковић 2009, 13).

Николић-Ристановић и Константиновић-Вилић (2018) издвајају следећу типологију криминалитета: криминалитет насиља, политички криминалитет, имовински криминалитет, привредни (економски) криминалитет, корупција, компјутерски криминалитет, саобраћајна делинквенција, професионални криминалитет, криминалитет белог оковратника, организовани криминалитет, трговина људима, малолетничка делинквенција, рецидивизам (повратништво) и криминалитет жена.

При реченом је потребно нагласити да не постоји унификована феноменолошка класификација криминалитета. Као пример може се навести и класификацију коју је дао Ђукић (2019), а према којој се могу усвојити комбиновани критеријуми поделе криминалитета на: „деликте насиља, имовинске деликте,

привредни криминалитет, организовани криминалитет, рачунарски криминалитет, саобраћајну деликвенцију, сексуалну деликвенцију, политички криминалитет, еколошку деликвенцију, малолетничку деликвенцију и рецидивизам” (99).

## Појам и карактеристике рачунарског криминалитета

Рачунарски криминалитет је данас „постао један од друштвено најопаснијих видова криминалитета, чија се стопа из дана у дан стално повећава” (Станковић, 2016, 48). У теорији не постоји јединствена дефиниција рачунарског криминалитета.

Рачунарски криминалитет је појава о којој се, од самог њеног настанка, у теорији, правосудној и законодавној пракси развијених држава и међународних институција, доста пише и говори. Разматрају се сви њени аспекти. Настоје се пружити што комплетнији одговори на многобројна, сваким даном све сложенија питања. Комплексност проблематике са којом смо преко четрдесет година суочени тек делимично се може наслутити кроз бројне радове из ове области. Упркос великом обиму материјала који обухвата теоријска разматрања, бројне примере из праксе, законска решења, као и различите међународне акте, јасно је да је реч о врло сложеној појави која захтева континуиран рад и едукативно усавршавање представника кривичноправне и криминалистичке праксе.

Рачунарски криминалитет представља облик „криминалног понашања код кога се коришћење компјутерске технологије и информатичких система испољава као начин извршења кривичног дела, или се компјутер употребљава као средство или циљ извршења, чиме се остварује нека у кривичноправном смислу релевантна последица” (Алексић и Шкулић 2007, 385). У контексту поменуте дефиниције, аутори су изнели и аргументацију исте, истичући карактеристике саме појаве које се морају имати у виду, као и основних елемената једне дефиниције. Па тако „одређивање појма компјутерског криминалитета се не може заснивати на утврђивању у оквиру његове дефиниције, елемената, који нису карактеристични за све облике овог вида делинквенције, као што су нпр. профил учинилаца, конкретна врста кривичног дела, врста штетне последице, мотив за криминално понашање, итд. Зато је приликом дефинисања компјутерског криминалитета неопходно имати веома широк приступ” (Алексић и Шкулић 2007, 385).

У смислу реченог, „једна свеобухватна и широка дефиниција компјутерског криминалитета мора заснивати на три основна елемента: 1. начину извршења, 2. средству извршења и 3. последици криминалног деловања. Начин извршења ових деликата се заснива на употреби компјутера, при чему само то коришћење рачунара може бити испољено као целовит *modus operandi*, или као један његов сегмент. Компјутер може бити и основно средство извршења ових кривичних дела, а потребно је поред тога да је на такав начин остварена и нека у кривичноправном смислу кажњива последица, с тим што последица

може бити испољена и на самим компјутерима, информатичкој, или комуникацијској мрежи” (Алексић и Шкулић 2007, 385).

Дефиниција прихваћена у Закону о организацији и надлежности државних органа за борбу против високотехнолошког криминала, упућује на одређење да „високотехнолошки криминал у начелу, представља вршење кривичних дела код којих се као објекат или средство извршења кривичних дела јављају рачунари, рачунарске системи, рачунарске мреже, рачунарске подаци, као и њихови производи у материјалном или електронском облику. Под производима у електронском облику се притом посебно подразумевају рачунарске програми и ауторска дела која се могу употребити у електронском облику” (ЗОНДОВК, 2005, чл. 2). Кривични законик опредељује неколико битних термина из ове области. Између осталих, одређује да је „рачунар сваки електронски уређај који на основу програма аутоматски обрађује и размењује податке, као и да је рачунарска систем сваки уређај или група међусобно повезаних или зависних уређаја од којих један или више њих, на основу програма, врши аутоматску обраду података” (КЗ, 2005, чл 112, тач. 33 и 34).

Значајна особина рачунарског криминалитета јесте велика феноменолошка разноврсност. Бројни су појавни облици злоупотреба рачунарске технологије, а с обзиром да је ова врста криминалитета у константном развоју и ширењу, свакодневно смо сведоци настанка нових, све сложенијих и опаснијих форми. То је и разумљиво јер се ради о технологији са великим могућностима и применом у скоро свим областима живота, те су и могућности за злоупотребу рачунара сваким даном све веће.

У најзначајније карактеристике рачунарског криминалитета се могу сврстати: 1) Просторна димензија криминалног деловања (корисници рачунарске технологије се без контроле могу кретати у виртуелном информатичком свету, без обзира на државне границе); 2.) Временска димензија криминалног деловања (захваљујући расположивим техничким могућностима и с обзиром на аутоматизовани амбијент, рачунарска криминална деловања се веома брзо реализује); 3.) Константно ширење на нове области друштвеног живота; 4.) Специфичан профил учиниоца (злоупотребом било ког елемента рачунарске технологије у већини случајева се баве лица која ту технологију добро и познају); 5.) Велика тамна бројка (тамна бројка неког недозвољеног понашања значи пре свега да не постоје поуздана сазнања о обиму, структури, динамици и другим важним показатељима значаја који иста представља за друштвену заједницу); 6.) Начин вршења и откривања криминалних радњи (реч је о веома развијеним техникама и изузетно осмишљеним активностима приликом злоупотребе података); 7.) Тежина последица и висина штета (штетна последица испољава се као настала имовинска штета, али исто тако може да се испољи у виду губљења поверења у сигурност и тачност добијених информација из компјутерског система, што може довести до различитог третирања и нарушавања пословног угледа многих привредних и ванпривредних субјеката); 8.) Вишеструка улога рачунарске технологије (рачунарска технологија се може појавити у вишеструкој улози, односно као: циљ напада, алат, окружење и доказ)” (Матијашевић 2013, 18-25).

Сагледавањем карактеристичних обележја рачунарског криминалитета, постаје донекле јасно због чега се све више у теорији разматрају многобројни аспекти ове друштвене појаве, и због чега се легислатива све већег броја држава мења у правцу све детаљнијег уређења наведене материје. Због свог специфичног карактера, високе стопе раста и великих потенцијалних могућности, ова врста криминала полако прераста у врло озбиљан национални и глобални проблем.

Имајући у виду значај рачунарског криминалитета у области кривичног права и криминалистике, у наставку ће бити више речи о неким најзначајнијим аспектима методике откривања кривичних дела из сфере рачунарског криминалитета.

### **Методика откривања кривичних дела из сфере рачунарског криминалитета**

Према важећем кривичном законодавству, кривична дела против безбедности рачунарских података, као најзначајнија кривична дела из области рачунарског криминалитета, сврстана су у поглавље XXVII Кривичног законика, чланови 298-304а. Законодавац је у групу кривичних дела против безбедности рачунарских података, у посебном делу Кривичног законика, уврстио следећа кривична дела: Оштећење рачунарских података и програма (чл. 298 КЗ), Рачунарска саботажа (чл. 299 КЗ), Прављење и уношење рачунарских вируса (чл. 300 КЗ), Рачунарска превара (чл. 301 КЗ), Неовлашћени приступ заштићеном рачунару, рачунарској мрежи и електронској обради података (чл. 302 КЗ), Спречавање и ограничавање приступа јавној рачунарској мрежи (чл. 303 КЗ), Неовлашћено коришћење рачунара или рачунарске мреже (чл. 304 КЗ), Прављење, набављање и давање другом средстава за извршење кривичних дела против безбедности рачунарских података (чл. 304а КЗ).

Према Станковићу (2016), „откривање, тумачење и доказно коришћење промена насталих у софтверу захтева изузетну стручност и ангажовање компјутерских експерата високог нивоа којих данас има веома мало, па то представља прворазредни проблем са којим се треба суочити. Најчешће се извршиоци ових кривичних дела налазе у једној држави, а нападају системе који се налазе у другим државама, па то ствара додатни проблем сарадњи са полицијом других држава у откривању извршиоца и обезбеђењу доказа” (50).

Имајући у виду узроке настанка и динамику развоја злоупотребе рачунарских технологија, можемо закључити да наше друштво поседује низ карактеристика и околности које погодују појави и развоју разних облика рачунарског криминалитета. Неки од ових узрока су: „непостојање позитивно-правне кривичне регулативе у односу на безбедност рачунарских података, до 2003. године; социо-економска ситуација у држави већ дужи низ година није стабилна; до ширег коришћења рачунарске технологије долази и на нивоу индивидуалних корисника, као и на нивоу државних и приватних организација, што има и своју негативну страну, јер са порастом броја корисника, а упоредо



и њихових знања и способности, расте и могућност за евентуалне злоупотребе; недовољно развијена култура коришћења рачунарске технологије која подразумева не само адекватна знања и способности корисника, већ и оријентисаност ка увођењу адекватне заштите рачунара” (Матијашевић 2013, 83-84).

Такође, неопходно је прецизно дефинисати и препознати профил извршилаца кривичних дела из сфере рачунарског криминала, „с обзиром на то да се ради о информатичким стручњацима који користе своје знање у погрешне сврхе. Иако се методологија и мотиви извршилаца разликују, најчешћи мотив јесте имовинска корист, мада је понекад то само доказивање у хакерском свету, слање одређене поруке друштву, појединцу, власти и слично, анализом основних особености извршилаца може се допринети одређивању ефикаснијих превентивних активности у области компјутерског криминалитета” (Матијашевић 2013, 236). Сходно овоме Бановић (2002) наводи да је „мотив значајна индицијална чињеница многих класичних облика криминалитета, па и компјутерских кривичних дела. Мотив као индиција, посебно долази до изражаја при постављању верзије о осумњиченом лицу, без обзира на то да ли је реч о једном учиниоцу, или о групи, па је тада методом елиминације потребно одстранити сумњу са невиних лица” (323).

Оно што рачунарски криминалитет чини примамљивим за потенцијалне извршиоце кривичних дела, јесте његова просторна неограниченост, изражена анонимност и брзина извршења. У том смислу, као ендегени фактори овог облика криминалитета јавља се фрустрација изазвана изузетно великим бројем информација доступним на интернету, унутрашња жеља ка лаком и брзом богаћењу, изолованост и социјална отуђеност која се јавља као последица интернет зависности и различити ментални поремећаји.

Природа информационих технологија „изузетно отежава откривање и доказивање, односно гоњење учинилаца ових кривичних дела. Рачунари и рачунарски системи повезани су на глобалном нивоу, што омогућава да се предузимају инкриминисане радње из једне државе у било којој другој држави, под условом да са обе стране постоји рачунар и интернет конекција. Висок степен анонимности корисника доприноси отежаном откривању извора криминалне активности од стране органа гоњења, док их границе територијалне надлежности, у одређеним случајевима, спречавају у процесуирању откривених учинилаца ових кривичних дела” (Писарић 2013, 292). Управо отежано откривање, компликовано доказивање и неефикасна превенција подстичу потенцијалне извршиоце ових кривичних дела на доношење одлуке о извршењу.

Дакле, „за рачунарски криминалитет карактеристично је тешко откривање и тешко прибављање доказа, а сам поступак разјашњавања и доказивања захтева посебан приступ, стручна знања и мултидисциплинарни аспект сагледавања ових кривичних дела, из чега произилази потреба стицања одговарајућих знања од стране оперативних радника полиције, јавних тужилаца, њихових заменика, истражних судија. Висок степен познавања рачунара, његових могућности и начина коришћења представља предуслов за откривање, кривично гоњење и суђење учиниоцима ових кривичних дела” (Суботин и Матијашевић Обрадовић 2019, 219).

Специјализоване јединице државних органа за сузбијање криминала „представљају неопходан сегмент у циљу сузбијања компјутерског криминалитета. Имајући у виду значај и количину информација која се налази у савременим компјутерским и другим комуникационим мрежама, неопходно је, поред ових специјализованих јединица и њиховог константног унапређења и едукације, развијати софтверске алате и пратити развој технологије како би се успоставила ефикаснија заштита, уз успешније откривање и сузбијање компјутерског криминала. Унапређена заштита у овој сфери доприноси стварању амбијента погодног за инвестиције и развој пословања привредних субјеката” (Милошевић 2007, 71).

Поред специјализације у погледу откривања и доказивања кривичних дела рачунарског криминалитета, неопходно је, како је већ наглашено, значајну пажњу посветити самој личности извршилаца ових кривичних дела.

Најчешћи начини долажења до сазнања о извршеном кривичном делу из области рачунарског криминалитета „јесу пријаве радника, анонимне и псеудонимне пријаве, или кроз вршење надзора и контроле” (Алексић и Миловановић 1994, 297).

Некада је откривање рачунарских кривичних дела „било знатно лакше управо због тога што је мањи број људи поседовао одговарајућа знања и вештине које би им омогућиле да компјутер користе у криминалне сврхе, а данас је проблематика откривања ових кривичних дела сложенија имајући у виду изузетно широк круг корисника компјутера. У пракси се показало да се многи облици компјутерског криминалитета открију тек када неко од учинилаца направи грешку или се кроз истраживање уочене грешке открије криминална делатност појединца или групе. У том смислу, све чешће се применом специјалних програма постављају одговарајуће „замке” које за циљ имају откривање учиниоца ових кривичних дела” (Суботин и Матијашевић Обрадовић 2019, 220).

## Закључак

Рачунарски криминалитет карактерише изузетна феноменолошка разноврсност која отежава његово јединствено и прецизно појмовно одређење, а перманентан интензивни развој рачунарских технологија доприноси константном проширивању појавних облика и поставља све веће изазове пред органе надлежне за његово сузбијање.

Такође, приступачност и релативно слаби заштитни механизми рачунарске технологије, затим, изражена анонимност као једна од кључних карактеристика рачунарског криминалитета, те легислативни третман кривичних дела из ове области који захтева сталне промене и усклађивање са европским стандардима, а свакако и неефикасна превенција у сфери високотехнолошког криминалитета у начелу, само су неки од фактора који доприносе константном расту броја кривичних дела из области рачунарског криминалитета.

Након краћег осврта на појам и значај криминалистике као науке, и криминалистичке методике као гране криминалистике, те појмовног одређења и основних карактеристика криминалитета уопште, и рачунарског криминалитета, у раду су анализирани најзначајнији аспекти методике откривања кривичних дела рачунарског криминалитета.

Поред специјализације у погледу откривања и доказивања кривичних дела рачунарског криминалитета, неопходно је значајну пажњу посветити самој личности извршилаца ових кривичних дела. У том смислу, мотив за извршење ових кривичних дела представља значајну индицијалну чињеницу. Такође, у пракси се показало да се многи облици рачунарског криминалитета открију тек када неко од учинилаца направи грешку или се кроз истраживање уочене грешке открије криминална делатност појединца или групе. Речено упућује на закључак да отежано откривање, компликовано доказивање и неефикасна превенција свакако подстичу потенцијалне извршиоце на доношење одлуке о предузимању радњи кривичних дела из ове области, што опет упућује у ком смеру се треба кретати у циљу отклањања потешкоћа у методици откривања и прикупљања доказа.

## Литература

1. Алексић, Живојин и Миловановић, Зоран. 1994. *Криминалистика*. Београд: Партенон.
2. Алексић, Живојин и Миловановић, Зоран. 1991. *Криминалистика*. Београд: Правни факултет Универзитета у Београду.
3. Алексић, Живојин и Шкулић, Милан. 2007. *Криминалистика*. Београд: Правни факултет Универзитета у Београду и Јавно предузеће „Службени гласник”.
4. Бановић, Божидар. 2002. *Обезбеђење доказа у криминалистичкој обради кривичних дела привредног криминалитета*. Београд: Виша школа унутрашњих послова.
5. Бјелајац, Жељко. 2013. *Организовани криминалитет, империја зла*, Нови Сад: Правни факултет за привреду и правосуђе.
6. Бјелајац, Жељко и Матијашевић, Јелена. 2014. „Значај борбе против корупције и организованог криминала у процесу придруживања земаља Западног Балкана Европској унији”. У: *Европска унија и Западни Балкан – изазови и перспективе*, ур. Драган Ђукановић и Владимир Трапара, 533-553. Београд: Институт за међународну политику и привреду.
7. Бошковић, Мићо и Бановић, Божидар. 1995. *Криминалистичка методика*. Београд: Виша школа унутрашњих послова.
8. Бошковић, Мићо. 2009. *Привредни криминалитет*, Бар: Факултет за пословни менаџмент.
9. Бошковић, Мило и Марковић, Милош. (2015). *Криминологија са елементима виктимологије*. Нови Сад: Правни факултет за привреду и правосуђе.
10. Ђукић, Станислав. 2019. „Методика откривања и доказивања кривичних дела класичног криминалитета”. *Војно дело* LXIX (6): 96-111.

11. Ђукић, Станимир. 2017. „Методика откривања и обезбеђење доказа у криминалистичкој обради кривичних дела привредног криминалитета”. *Војно дело* LXVII (6): 139-165.
12. Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала [ЗОНДОВК], „Службени гласник Републике Србије”, бр. 61/05 и 104/09.
13. Кривични законик [КЗ], „Службени гласник Републике Србије”, бр. 85/2005, 88/2005 - испр., 107/2005 - испр., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 и 35/2019.
14. Матијашевић, Јелена. 2013. *Кривичноправна регулатива рачунарског криминалитета*. Нови Сад: Правни факултет за привреду и правосуђе.
15. Матијашевић, Јелена, Бјелајац, Жељко и Димитријевић, Душко. 2012. „Конвенција Савета Европе о високотехнолошком криминалу”. *Европско законодавство* XI (42): 37-52.
16. Матијашевић, Јелена, Бингулац, Ненад и Драгојловић, Јоко. 2015. „Улога интернета у сфери образовања”. *Педагошка стварност* VXI (3): 393-403.
17. Матијашевић, Јелена. 2008. „Организовани криминалитет – појам, карактеристике, узроци и методе супротстављања”. *Право-теорија и пракса* XXV (1-2): 80-89.
18. Matijašević, Jelena i Zarubica, Sara. 2021. „Smuggling and Illegal Trade as forms of Economic Crime”. *Pravo – teorija i praksa*, XXXVIII (3): 28-41.
19. Matijašević, Jelena. 2012. „The importance of preventive acting in the field of crime suppression with the reference to strategic acts of the Western Balkan countries”. *The Review of International Affairs*, LXIII (1148), 52-70.
20. Матијевић, Миле, Шушљик, Недељко и Шарчевић, Зоран. 2020. *Увод у криминалистику*. Бања Лука: Универзитет ПИМ.
21. Матијевић, Миле и Марковић, Милош. 2013. *Криминалистика*. Нови Сад: Правни факултет за привреду и правосуђе.
22. Милошевић, Милан. 2007. „Актуелни проблеми сузбијања компјутерског криминала”. *Наука, безбедност, полиција - Журнал за криминалистику и право*, XII (1): 57-74.
23. Николић-Ристановић, Весна и Констатиновић-Вилић, Слободанка. 2018. *Криминологија*. Београд: Прометеј.
24. Писарић, Милена. 2013. „Потребни нормативни одговор на проблеме откривања и доказивања дела високотехнолошког криминала”. *Зборник радова Правног факултета*, XLVII (1): 291-307.
25. Радовић, Владета. 2008. „Медији и е-образовање”. *Социјална мисао* XV (2): 129-145.
26. Станковић, Недељко. 2016. *Увод у криминалистику*. Брчко: Европски универзитет.
27. Суботин, Маја и Матијашевић-Обрадовић, Јелена. 2019. „Криминолошки и криминалистички аспект рачунарског криминалитета”. У: *Право и дигиталне технологије*, ур. Марко Царић, 212-222. Нови Сад: Правни факултет за привреду и правосуђе.

## **METHODOLOGY OF DETECTION OF COMPUTER CRIME OFFENSES**

**Summary:** Computer crime is characterized by an exceptional phenomenological diversity that complicates its unique and precise conceptual definition, and the permanent intensive development of computer technologies contributes to the constant expansion of its forms and poses increasing challenges to the authorities responsible for combating it. After a brief review of the concept and importance of criminology as a science, and criminological methodology as a branch of criminology, and the conceptual definition and basic characteristics of crime in general, and computer crime, the paper analyzes the most important aspects of crime detection methodology in this area. The conclusion is that the basic characteristics of computer crime, difficult detection, complicated proving and ineffective prevention certainly encourage potential perpetrators to make a decision on taking criminal acts in this area, which again indicates in which direction to move in order to eliminate difficulties in the methodology of detection and collection of evidence in criminal offenses of computer crime.

**Key words:** Computer Crime, Criminalistics, Criminalistic Methodology, Criminal Code, Criminal offenses

